BIURO BEZPIECZEŃSTWA NARODOWEGO

PROJEKT, 24 lipca 2015r.

DOKTRYNA BEZPIECZEŃSTWA INFORMACYJNEGO RP

Warszawa, 2015

SPIS TREŚCI

Wprowadzenie 3
1. Cele strategiczne RP w dziedzinie bezpieczeństwa informacyjnego 5
2. Środowisko bezpieczeństwa informacyjnego RP 6
2.1 Wymiar wewnętrzny 6
2.1.1 Zagrożenia 6
2.1.2 Wyzwania (ryzyka i szanse) 6
2.2 Wymiar zewnętrzny 7
2.2.1 Zagrożenia 7
2.2.2 Wyzwania (ryzyka i szanse) 8
3. Koncepcja zadań operacyjnych w dziedzinie bezpieczeństwa informacyjnego RP 9
4. Koncepcja zadań preparacyjnych (przygotowawczych) w dziedzinie bezpieczeństwa informacyjnego (utrzymanie i rozwój systemu bezpieczeństwa informacyjnego RP) 12
4.1. Podsystem kierowania 12
4.2. Ogniwa operacyjne 13
4.3. Publiczne i prywatne ogniwa wsparcia 14
Zakończenie 15

WPROWADZENIE

1. Bezpieczeństwo informacyjne – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo - jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mającym charakter transsektorowy i wpływającym na efektywność funkcjonowania całego systemu bezpieczeństwa.

2. Działania na rzecz bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem ochrony praw człowieka i obywatela, a szczególnie poszanowaniem prawa do wolności słowa oraz prywatności. Proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka.

3. Punktem wyjścia niniejszej Doktryny są kierunkowe postanowienia Strategii Bezpieczeństwa Narodowego RP dotyczące bezpieczeństwa informacyjnego i ochrony informacji niejawnych oraz cyberbezpieczeństwa. Ten ostatni wymiar bezpieczeństwa informacyjnego został już wcześniej rozwinięty w przyjętej w 2015 r. Doktrynie cyberbezpieczeństwa RP i w niniejszym dokumencie nie będzie szerzej podejmowany. W przyszłości należałoby scalić obydwa dokumenty w jeden.

4. Główne pojęcia przyjęte w Doktrynie bezpieczeństwa informacyjnego RP:

   - **Bezpieczeństwo informacyjne państwa -** transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizację takich zadań jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego.

   - **Środowisko bezpieczeństwa informacyjnego** (przestrzeń informacyjna, infosfera) – zewnętrzne i wewnętrzne, militarne i niemilitarne (cywilne), osobowe, technologiczne i organizacyjne warunki bezpieczeństwa (warunki realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa informacyjnego i osiągania ustalonych przezeń celów w tym zakresie), charakteryzowane przy pomocy takich kategorii, jak zagrożenia, wyzwania oraz szanse i ryzyka:

     - **zagrożenia bezpieczeństwa informacyjnego** – pośrednie lub bezpośrednie, zakłócające lub destrukcyjne oddziaływania na podmiot;

     - **wyzwania bezpieczeństwa informacyjnego** – sytuacje problemowe w obszarze bezpieczeństwa informacyjnego, stwarzane zwłaszcza przez szanse i ryzyka oraz generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw w tym zakresie;

     - **szanse bezpieczeństwa informacyjnego** – niezależne od woli podmiotu okoliczności (zjawiska i procesy w środowisku bezpieczeństwa informacyjnego) sprzyjające realizacji interesów oraz osiąganiu celów podmiotu w obszarze bezpieczeństwa informacyjnego;

     - **ryzyka bezpieczeństwa informacyjnego** – niebezpieczne dla funkcjonowania w przestrzeni informacyjnej konsekwencje przyszłych własnych działań.

   - **Komunikacja strategiczna –** synteza działań informacyjnych danego podmiotu strategicznego (np. państwa, sojuszu, koalicji) ukierunkowanych na kształtowanie poglądów, ocen, opinii itp. oraz decyzji innych podmiotów z otoczenia strategicznego (podległych, współdziałających, neutralnych, konkurujących, wrogich) w sposób korzystny dla własnych interesów strategicznych. Realizowana jest poprzez aktywność w takich obszarach, jak: dyplomacja publiczna, komunikacja społeczna, operacje informacyjne oraz operacje psychologiczne.

   - **Dyplomacja publiczna** – część dyplomacji danego państwa realizowana w publicznej przestrzeni informacyjnej jako forma pozytywnego wpływania na postawy społeczne w innych krajach i kształtowania w ten sposób polityki zagranicznej danego państwa.

Cechą szczególną dyplomacji publicznej jest wykorzystywanie środków wykraczających poza zakres tradycyjnie pojmowanej dyplomacji, a jej istotnym elementem jest kształtowanie opinii publicznej w innych krajach przy pomocy mechanizmów wykorzystywanych przez marketing gospodarczy oraz polityczny.

- **Komunikacja społeczna** proces wytwarzania, przekształcania i przekazywania informacji między jednostkami, grupami i organizacjami społecznymi, mający na celu dynamiczne kształtowanie, modyfikację bądź zmianę wiedzy, postaw i zachowań w kierunku zgodnym z wartościami i interesami oddziałujących na nie podmiotów. W komunikacji społecznej nadawca w przekazie może wykorzystywać środki perswazji lub manipulacji medialnej w celu wywołania określonego zachowania u odbiorcy.
- **Operacje informacyjne (walka informacyjna)** czynności polegające na oddziaływaniu na informacje i/lub systemy informacyjne w celu kształtowania i przejmowania procesów decyzyjnych przeciwnika (zautomatyzowanych oraz z udziałem czynnika ludzkiego), przy jednoczesnej ochronie własnych procesów decyzyjnych; w wymiarze wojskowym także działalność mająca na celu wywarcie pożądanego wpływu na wolę, rozumienie i zdolności przeciwników, potencjalnych przeciwników lub innych stron konfliktu, wspierających cele danej misji; w operacjach informacyjnych można wyróżnić działania ofensywne i defensywne:
  - **do działań ofensywnych** należy zaliczyć: operacje psychologiczne, pozorację, destrukcję, walkę elektroniczną, atak informatyczny, działania z zakresu komunikacji społecznej;
  - **do działań defensywnych** należy zaliczyć: bezpieczeństwo informacyjne, osłonę, działania kontrpropagandowe, działania kontrwywiadowcze, walkę elektroniczną, informacyjne działania specjalne.
- **Operacje psychologiczne** – operacje mające na celu wpływanie na emocje, motywacje, obiektywne rozumowanie, a ostatecznie zachowanie rządów państw obcych, organizacji, grup i osób będących celami tych operacji, tak aby osiągnąć efekt w postaci wzmocnienia lub nakłonienia do zachowań korzystnych dla realizacji własnych interesów. Mogą być wykorzystywane zarówno w czasie pokoju (klęsk żywiołowych, stanów kryzysowych i alarmowych), jak i podczas wojny.
- **Inżynieria społeczna** – zespół metod i środków celowego manipulowania społeczeństwem.
- **Propaganda, dezinformacja –** rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń.
- **Manipulacja informacją –** wykorzystanie prawdziwych informacji, ale w taki sposób, żeby wywołać fałszywe implikacje, np. drogą pomijania niektórych, istotnych, ale niewygodnych informacji lub poprzez taki dobór informacji, żeby budziły fałszywe skojarzenia.
- **Trollowanie** (trolling) – antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych, polegające na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów.

1. CELE STRATEGICZNE RP W DZIEDZINIE BEZPIECZEŃSTWA INFORMACYJNEGO

1. Interesem narodowym w obszarze bezpieczeństwa informacyjnego jest dysponowanie skutecznym narodowym potencjałem bezpieczeństwa zapewniającym gotowość i zdolność do zapobiegania zagrożeniom występującym w przestrzeni informacyjnej (infosferze, infoprzestrzeni), w tym odstraszania, obrony i ochrony przed nimi oraz likwidowania ich następstw.

2. Celem strategicznym w obszarze bezpieczeństwa informacyjnego jest zapewnienie bezpiecznego funkcjonowania RP w przestrzeni informacyjnej, z uwzględnieniem bezpieczeństwa informacyjnego struktur państwowych (zwłaszcza administracji publicznej, służb bezpieczeństwa i porządku publicznego, służb specjalnych i sił zbrojnych), sektora prywatnego i społeczeństwa obywatelskiego.

3. Cele strategiczne osiąga się poprzez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Głównym celem operacyjnym jest panowanie we własnej przestrzeni informacyjnej (infosferze) oraz selektywna obrona interesów narodowych w zewnętrznej (obcej) przestrzeni informacyjnej (infosferze). Osiąga się go poprzez realizacje takich zadań, jak:

   - utrzymywanie i demonstrowanie gotowości do przeciwdziałania zagrożeniom informacyjnym;
   - rozpoznanie, analiza i ocena zagrożenia informacyjnego;
   - ochrona strategicznych zasobów informacyjnych państwa;
   - reagowanie na zagrożenia i podejmowanie działań ofensywnych w zakresie walki informacyjnej;
   - kształtowanie świadomości społecznej w zakresie celów polityki informacyjnej państwa oraz interesu narodowego;
   - bieżące rozpoznanie systemu wartości oraz słabych stron przeciwnika.

4. Do osiągnięcia celów operacyjnych niezbędne jest, w wymiarze preparacyjnym, zbudowanie, utrzymywanie i systematyczne doskonalenie (rozwój) zintegrowanego, zarządzanego (koordynowanego) ponadresortowo, systemu bezpieczeństwa informacyjnego RP obejmującego:

   - podsystem kierowania – zdolny do organizowania i koordynowania działań podmiotów rządowych i pozarządowych realizujących zadania w zakresie bezpieczeństwa informacyjnego;
   - podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia działań defensywnych (ochronnych i obronnych) oraz ofensywnych w zakresie bezpieczeństwa informacyjnego i walki informacyjnej, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych.

2. ŚRODOWISKO BEZPIECZEŃSTWA INFORMACYJNEGO RP

2.1. WYMIAR WEWNĘTRZNY

2.1.1. Zagrożenia

5. Zagrożeniem płynącym z funkcjonowania w środowisku informacyjnym może być rozpowszechnianie i powielanie treści propagandowych mające na celu ukazanie polskiej racji stanu w negatywnym świetle, co *de facto* szkodzi interesowi państwa (stosowanie prowokacji, celowe manipulowanie przekazem poprzez wyrywanie z kontekstu fragmentów wypowiedzi polityków RP, nadawanie im kontrowersyjnego charakteru).

6. Do najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
   - występowanie w społeczeństwie deficytów informacyjnych, skutkujących podatnością na wrogą perswazję;
   - potencjalna dezinformacja obywateli poprzez agresywne działania propagandowe; dywersja ideologiczna – narzucanie obcych idei niezgodnych z interesem państwa;
   - pojawienie się i rozwój postaw antypaństwowych; nasilenie się postaw agresywnych, defetystycznych (np. islamofobia, szpiegomania);
   - wzrost negatywnych postaw społecznych lub wystąpienie konfliktów społecznych, zgodnych z intencjami przeciwnika informacyjnego (informacyjnego napastnika);
   - istnienie (tworzenie) agentury wpływu (inspirowanie do zakładania oraz wsparcie finansowe formacji politycznych lub organizacji społecznych wspierających i realizujących obce interesy w Polsce);
   - wpływanie na opinię publiczną przez agentów zmiany sterowanych z zewnątrz, zwłaszcza aktywizacja wybranych grup społecznych przez inne państwo oraz realizacja interesów obcych państw, sprzecznych z interesem RP;
   - obniżanie się morale społeczeństwa w razie agresji informacyjno-propagandowej, rzutujące negatywnie na polityczno-militarne procesy decyzyjne.

7. Do zagrożeń informacyjnych związanych z funkcjonowaniem w cyberprzestrzeni należą:
   - dezinformacja, trolling, wroga propaganda, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego;
   - ataki powodujące zakłócenia funkcjonowania sieci teleinformatycznych w sektorach i instytucjach o podwyższonym stopniu wrażliwości, w tym tworzących infrastrukturę krytyczną;
   - istnienie technologicznych luk, które dają szansę, także niezauważonej, ingerencji w treści portali internetowych oraz wpływania na zdolności do działania w cyberprzestrzeni.

8. Odrębnym obszarem występowania potencjalnych zagrożeń jest przestrzeń medialna:
   - monopolizacja rynku informacyjnego i jego poszczególnych struktur oraz niekontrolowany rozwój rynku informacyjnego media masowe mogą być narzędziem dezinformacji;
   - przejmowanie lub finansowanie mediów przez podmioty nieprzychylne lub wrogie Polsce;
   - pojawienie się w przestrzeni informacyjnej mediów propagujących idee sprzeczne z interesem narodowym;
   - aktywne uczestnictwo przeciwnika w polskich mediach społecznościowych – propagowanie idei sprzecznych z interesem narodowym;
   - nieświadome, niezamierzone powielanie przekazu informacyjnego sprzecznego z interesem narodowym przez użytkowników mediów społecznościowych lub media masowe.

9. Poważnym zagrożeniem może okazać się eksploatowanie drażliwych kwestii w kontaktach międzynarodowych, w tym bilateralnych, przy wykorzystaniu wsparcia określonych podmiotów i osób.

2.1.2. Wyzwania (ryzyka i szanse)

10. Istotnym ryzykiem w obszarze bezpieczeństwa informacyjnego może być niewystarczająca adaptacja strukturalna i koordynacyjna działań w obliczu zagrożenia informacyjnego, szczególnie w kreowaniu spójnej polityki informacyjnej oraz działań w zakresie bezpieczeństwa informacyjnego.

11. Ryzyka systemowe (odnoszące się do niedoskonałego funkcjonowania podsystemu bezpieczeństwa informacyjnego państwa):
    - brak właściwej ochrony własnych militarnych systemów informacyjnych i ocen słabości systemów informacyjnych potencjalnych przeciwników;
    - brak efektywnego systemu kształcenia i szkolenia w zakresie bezpieczeństwa informacyjnego;
    - niewystarczająca liczba wykwalifikowanych pracowników bezpieczeństwa informacyjnego;
    - brak jednolitego, skoordynowanego przekazu informacyjnego ze strony struktur rządowych formułowanego do społeczeństwa;
    - brak systemu finansowania przedsięwzięć na rzecz zapewnienia bezpieczeństwa informacyjnego;
    - niska reaktywność systemowa wobec agresji informacyjno-propagandowej;
    - nieadekwatne do zagrożeń wzorce doktrynalne.

12. Ryzykiem w dziedzinie bezpieczeństwa informacyjnego może być podejmowanie przez organy państwa decyzji na podstawie informacji niepełnych, niesprawdzonych lub dezinformacji.
13. Źródłem ryzyk może okazać się również dysonans informacyjny różnych ośrodków informacyjnych.
14. Naruszenia praw i wolności obywateli w zakresie prawa do prywatności.
15. Szansę stanowić może potencjał społeczeństwa obywatelskiego, który można wykorzystać na rzecz zwiększenia bezpieczeństwa informacyjnego.
16. Wykorzystanie potencjału informacyjnego państwa w ramach systemu bezpieczeństwa narodowego stanowi szansę na zwiększenie efektywności działań w obszarze bezpieczeństwa informacyjnego.
17. Zdobywanie wiedzy o naturze i skutkach zagrożeń informacyjnych dla funkcjonowania państwa może stanowić szansę na efektywne dostosowanie wykorzystywanych sił i środków.
18. Do szans zaliczyć należy także rozwój potencjału naukowego oraz wzrost konkurencyjności ośrodków informacyjnych.

2.2. WYMIAR ZEWNĘTRZNY

2.2.1. Zagrożenia

19. Wśród podstawowych zagrożeń w obszarze bezpieczeństwa informacyjnego państwa należy wskazać takie jak:
    - deformowanie treści oraz wprowadzanie do systemów informacyjnych nieprawdziwych treści logicznych za pośrednictwem kanałów łączności rządowej czy wojskowych systemów dowodzenia;
    - działalność służb specjalnych i podmiotów informacyjnych innych państw oraz aktorów niepaństwowych (w tym szpiegostwo);
    - wroga aktywność operacyjna struktur informacyjno-propagandowych aktorów państwowych i pozapaństwowych;
    - działania propagandowe i dezinformacyjne;
    - dominacja potencjalnych agresorów w środowisku informacyjnym;
    - penetracja środowiska informacyjnego RP przez wrogie struktury informacyjno-propagandowe;
    - utrata zdolności wpływania, dystrybucji informacji w środowisku informacyjnym.

20. Poważnym zagrożeniem są niepożądane, zewnętrzne oddziaływania informacyjne, mogące dotyczyć procedur sterowania procesami decyzyjnymi państwa, na które ukierunkowany jest atak informacyjny.
21. Skutkować to może bezpośrednim przełożeniem na koncepcje doktrynalne odnoszące się do infrastruktury wojskowej, systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych.
22. Wśród najpoważniejszych zagrożeń związanych z niedoskonałym funkcjonowaniem społeczeństwa obywatelskiego należy zaliczyć:
    - inspirowane z zewnętrz działania informacyjne podmiotów wewnętrznych mające na celu wywoływanie i pogłębianie podziałów społecznych i politycznych;
    - wsparcie zewnętrzne dla podmiotów realizujących politykę przeciwnika;
    - dezinformacja obywateli innych państw, w tym tworzących wspólnoty organizacyjne w kwestiach dotyczących polskiej polityki zagranicznej.

23. Wśród istotnych zagrożeń związanych z funkcjonowaniem RP w wymiarze międzynarodowym wymienić należy:
    - doprowadzenie do eskalacji napięć w stosunkach międzynarodowych, w tym bilateralnych i multilateralnych;
    - kształtowanie negatywnego obrazu Polski na arenie międzynarodowej, w tym wśród sojuszników, przede wszystkim w ramach NATO i UE;
    - wywoływanie w społeczeństwach i elitach politycznych tych państw nastrojów antypolskich na przykład poprzez nagłaśnianie i akcentowanie jednostkowych wypowiedzi przedstawicieli polityki, sprzecznych z oficjalną linią polityki zagranicznej RP w kluczowych, strategicznych sprawach;
    - dyskredytowanie polskiej polityki zagranicznej na arenie międzynarodowej;
    - działanie zagranicznych struktur informacyjnych przeciwko interesom RP;
    - szerzenie treści antypolskich za pośrednictwem mediów o zasięgu międzynarodowym:
        - tworzenie w obiegu informacyjnym na Zachodzie obrazu Polski jako kraju ksenofobicznego i antysemickiego;
        - inspirowanie konfliktu polsko-litewskiego na tle mniejszości polskiej na Litwie – możliwość tworzenia przez wrogie służby specjalne wrażenia istnienia zbrojnego separatyzmu polskiego na Wileńszczyźnie;
        - inspirowanie konfliktu polsko-ukraińskiego na tle historycznym przy możliwym zastosowaniu zamachów terrorystycznych rzekomo dokonanych przez Ukraińców przeciw Polakom i odwrotnie;
    - budowanie lobby interesów obcego państwa w ramach struktur wspólnotowych (UE, NATO).
24. W związku z funkcjonowaniem RP w globalnej cyberprzestrzeni mogą pojawić się zagrożenia w postaci ataków cybernetycznych na instytucje rządowe, pozarządowe i kulturalne kształtujące świadomość narodową lub blokady rządowego przekazu informacyjnego wskutek ataków cybernetycznych.

2.2.2. Wyzwania (ryzyka i szanse)

25. Ryzyko systemowe (odnoszące się do niedoskonałości funkcjonowania podsystemu bezpieczeństwa informacyjnego w skali międzynarodowej i krajowej) odnosi się do niskiej reaktywności i niewystarczającej koordynacji działań sojuszników RP w obliczu zagrożeń informacyjnych oraz potencjalnego wpływu niezrzeszonych państw na decyzje i kierunek polityki wspólnotowej i sojuszniczej.
26. Ryzyka mogą wypływać z niewłaściwego zarządzania sytuacjami kryzysowymi wynikającymi z szerzenia treści antypolskich za pośrednictwem mediów o zasięgu międzynarodowym:
    - konieczność walki z wizerunkiem „antysemickiej Polski”;
    - osłabienie pozycji Polski na arenie międzynarodowej, w tym w ramach NATO i UE, do izolacji włącznie;
    - dyskredytacja władz RP w celu obniżenia ich pozycji w stosunkach z przywódcami innych państw.
27. Szansą w zapewnieniu bezpieczeństwa informacyjnego może być rozwinięcie współpracy bilateralnej i regionalnej w kwestii zwalczania zagrożeń dla bezpieczeństwa informacyjnego:
    - nawiązanie ścisłej współpracy z odpowiednimi instytucjami ukraińskimi, wpływanie na ich kształt i kierunki działania;
    - nawiązanie ścisłej współpracy z odpowiednimi instytucjami litewskimi, wpływanie na ich kształt i kierunki działania;
    - wzmacnianie potencjału informacyjnego NATO;
    - wykorzystanie działań reformujących WPZiB UE, w tym przyjęcia nowej Strategii Bezpieczeństwa UE;
    - aktywna polityka informacyjna RP na forach międzynarodowych.

3. KONCEPCJA ZADAŃ OPERACYJNYCH W ZAKRESIE BEZPIECZEŃSTWA INFORMACYJNEGO RP

28. Zadania operacyjne w zakresie efektywności walki informacyjnej powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego, obywatelskiego oraz w wymiarze transsektorowym.

29. W ramach opracowania zadań operacyjnych niezbędne jest wskazanie mechanizmów przeciwdziałania wykorzystywaniu wojny informacyjnej w celach polityczno-wojskowych naruszających prawo międzynarodowe oraz przeprowadzania wrogich działań i aktów agresji stanowiących zagrożenie dla międzynarodowego bezpieczeństwa i stabilności strategicznej.

30. Do głównych zadań sektora publicznego w wymiarze krajowym należą:

- rozpoznawanie środowiska informacyjnego (m.in. określenie podmiotów przyjaznych, neutralnych i wrogich) oraz analiza i ocena zagrożeń środowiska informacyjnego (w tym potencjalnych celów oraz możliwych do użycia kanałów informacyjnych);
- prognoza skuteczności planowanych działań;
- prowadzenie analizy ryzyka i prognoz dotyczących zagrożeń dla bezpieczeństwa informacyjnego;
- opracowanie systemu monitoringu potencjalnych zagrożeń oraz efektywnego systemu przeciwdziałania zidentyfikowanym zagrożeniom, w tym wymiany danych i informacji;
- współpraca z sektorem prywatnym w zakresie przeciwdziałania zagrożeniom;
- planowanie użycia środków oddziaływania na środowisko informacyjne;
- właściwe wykorzystywanie synergii powstałej w wyniku współpracy i koordynacji działań pomiędzy podmiotami różnych sektorów bezpieczeństwa narodowego i społeczeństwa obywatelskiego;
- wdrożenie efektywnego i akceptowalnego społecznie systemu identyfikacji źródeł przekazów informacyjnych;
- zapewnienie funkcjonowania spójnego systemu monitorowania i dystrybucji informacji w wymiarze cywilnym i wojskowym;
- wspieranie działań mających na celu umacnianie tożsamości narodowej;
- prowadzenie kampanii społecznych mających pozytywnie wpłynąć na obraz Polski; podejmowanie walki z propagandą ukazującą Polskę w negatywnym kontekście;
- działania z zakresu komunikacji społecznej budujące markę RP; wykorzystanie potencjału dyplomacji publicznej;
- prowadzenie działań zmierzających do zabezpieczenia informacyjnego strategicznych organizacji i spółek, których działanie wpływa bezpośrednio lub pośrednio na stan bezpieczeństwa narodowego Polski;
- zapobieganie, w ramach działań kontrwywiadowczych, aktywizacji przez obce państwo wybranych grup społecznych, celem realizacji interesów sprzecznych z interesem RP;
- stworzenie społecznej zdolności do rozpoznawania i neutralizacji dezinformacji; aktywizacja kapitału społecznego;
- wdrażanie mechanizmów kontrinformacji oraz edukacja i uświadamianie obywateli na poziomie narodowym m.in. poprzez zaangażowanie mediów;
- planowanie użycia i produkcji środków oddziaływania na środowisko informacyjne.

31. Główne zadania sektora publicznego na poziomie międzynarodowym:

- aktywne uczestnictwo w projektach i przedsięwzięciach międzynarodowych na rzecz bezpieczeństwa informacyjnego, organizowanych zarówno w ramach NATO jak i UE oraz innych organizacji, których Polska jest aktywnym członkiem i które są zgodne z interesem narodowym;
- prowadzenie aktywnej, jednolitej i spójnej polityki zagranicznej RP na forach międzynarodowych (szczególny nacisk na spójny przekaz informacyjny instytucji w kluczowych dla kraju kwestiach);

- wspieranie procesów służących wzmocnieniu bezpieczeństwa informacyjnego Sojuszu Północnoatlantyckiego i UE;
- gromadzenie wiedzy i doświadczeń oraz porównywanie narodowych regulacji z rozwiązaniami stosowanymi przez inne państwa, dotyczących działań z zakresu bezpieczeństwa informacyjnego;
- wymiana doświadczeń i dobrych praktyk oraz wykorzystanie wsparcia informacyjnego partnerów/sojuszników na arenie międzynarodowej;
- udział w międzynarodowym reagowaniu na zagrożenia bezpieczeństwa informacyjnego;
- efektywne funkcjonowanie w sojuszniczym systemie komunikacji strategicznej, w tym wymiana informacji w zakresie zagrożeń o charakterze globalnym;
- właściwe wykorzystywanie synergii powstałej w wyniku koordynacji działań rozproszonych (współpracy międzynarodowej);
- odpowiednie wykorzystywanie potencjału dyplomacji publicznej poszczególnych państw;
- objęcie mniejszości polskiej w regionie powszechnym dostępem do wszystkich polskich mediów elektronicznych (radio i tv); tworzenie silnej konkurencji dla mediów rosyjskich jako głównego przekaźnika informacji (propagandy) dla tej grupy ludności; współdziałanie z krajami regionu w zakresie nadawania programów radiowych i telewizyjnych na Białorusi;
- dotarcie z polskimi programami informacyjnymi (radiowymi i telewizyjnymi) do mniejszości polskiej w innych krajach; objęcie tej mniejszości programami edukacyjnymi w zakresie historii i współczesnej polityki;
- stały monitoring przekazu propagandowego ukierunkowanego na Polskę i treści dyskredytujących polską politykę zagraniczną; analiza pozwalająca identyfikować źródła przekazu oraz - na ile to możliwe - eliminowanie źródeł dezinformacji;
- budowa i utrwalenie wizerunku Polski na arenie międzynarodowej jako podmiotu przewidywalnego, o określonych zdolnościach, m.in. do budowania koalicji w zakresie rozwiązań będących we wspólnym interesie kilku państw;
- przeciwdziałanie dezinformacji w ramach obowiązującego prawa, merytoryczna i przekonująca argumentacja polskiej narracji na forach międzynarodowych, akcentująca zaangażowanie RP we wspólne projekty.

32. Główne zadania sektora prywatnego:

- współpraca z sektorem publicznym w zakresie przeciwdziałania zagrożeniom środowiska informacyjnego;
- włączenie prywatnych nadawców komercyjnych do realizacji zadań informacyjnych stawianych mediom publicznym wobec mniejszości polskiej np. na Litwie (system zachęt i ulg podatkowych);
- udział w mechanizmach wymiany informacji, szkoleniach, oraz stosowanie zasad dobrych praktyk;
- aktywność i rzetelność informacyjna wobec organów odpowiedzialnych za nadzór nad funkcjonowaniem strategicznych organizacji oraz spółek państwa.

33. Główne zadania sektora obywatelskiego:

- działania wspierające bezpieczeństwo informacyjne państwa (udział w zapewnianiu bezpieczeństwa sektora publicznego i prywatnego);
- kreowanie spójnego przekazu służącego interesom Polski;
- zaangażowanie obywateli oraz udział w przedsięwzięciach i ruchach obywatelskich służących wzmocnieniu bezpieczeństwa informacyjnego;
- samoorganizacja społeczeństwa obywatelskiego poprzez samokształcenie, podnoszenie świadomości o zagrożeniach i wspieranie obywatelskiego potencjału przeciwdziałania (np. tzw. „dobre trolle”);

- świadome konsumowanie treści informacyjnych, analiza treści (identyfikacja ataków propagandowych i dezinformacyjnych).

34. Główne zadania transsektorowe:

- wypracowanie mechanizmów efektywnej współpracy transsektorowej;
- bieżąca analiza środowiska bezpieczeństwa informacyjnego państwa;
- transsektorowa koordynacja realizacji zadań podmiotów sektora publicznego i prywatnego w dziedzinie walki informacyjnej;
- doskonalenie systemu przeciwdziałania zidentyfikowanym zagrożeniom w obszarze bezpieczeństwa informacyjnego, w tym wymiany danych i kluczowych informacji;
- angażowanie kluczowych komunikatorów w propagowanie jednolitego przekazu;
- współpraca sektora państwowego (służby, wojsko, administracja na wszystkich szczeblach) z mediami w celu lepszej ochrony interesów państwa w sferze informacyjnej;
- przeciwdziałanie propagandzie oraz reagowanie kryzysowe z wykorzystaniem potencjału społecznego;
- właściwe kreowanie postaw społecznych na rzecz bezpieczeństwa narodowego;
- ustanawianie standardów i dobrych praktyk służących osiąganiu celów strategicznych w zakresie bezpieczeństwa informacyjnego.

4. KONCEPCJA ZADAŃ PREPARACYJNYCH (PRZYGOTOWAWCZYCH) W DZIEDZINIE BEZPIECZEŃSTWA INFORMACYJNEGO (UTRZYMANIE I ROZWÓJ SYSTEMU BEZPIECZEŃSTWA INFORMACYJNEGO RP)

35. Podstawowym zadaniem preparacyjnym określającym kierunek działania w zakresie utrzymania i rozwoju systemu bezpieczeństwa informacyjnego RP jest integracja systemu walki informacyjnej, jako elementu w systemu bezpieczeństwa narodowego, przede wszystkim poprzez utrzymywanie i doskonalenie instytucji służących realizacji zadań w zakresie bezpieczeństwa informacyjnego.

36. Aby było to możliwe, konieczne jest dokonanie stosownej reformy regulacji w polskim systemie legislacyjnym, z uwzględnieniem zagadnień takich jak:

- stworzenie prawnych podstaw instytucjonalnej koordynacji działań w zakresie bezpieczeństwa informacyjnego;
- opracowanie rozwiązań umożliwiających przeciwdziałanie zagrożeniom informacyjnym przez właściwe podmioty (zdolności ofensywne i defensywne);
- opracowanie i wdrożenie norm regulujących relacje państwa, mediów publicznych i innych ośrodków informacyjnych w zakresie bezpieczeństwa informacyjnego RP.

37. Zbudowanie kompleksowego systemu umożliwiającego realizację zadań z zakresu polityki informacyjnej państwa (sektora cywilnego i militarnego).

38. Stworzenie (lub wykorzystanie istniejącego) organu pomocniczego Rady Ministrów o kompetencjach doradczych, konsultacyjnych i koordynacyjnych, odpowiedzialnego za analizę zagrożeń i opracowywanie zasad bieżącej i długofalowej polityki informacyjnej państwa.

39. Doskonalenie procedur, zasad i norm zmierzających do usprawnienia pracy organów odpowiedzialnych za ochronę obywateli w zakresie bezpieczeństwa informacyjnego.

40. Zabezpieczenie finansowe działań służących prowadzeniu polityki informacyjnej państwa.

41. Polskie rozwiązania w zakresie bezpieczeństwa informacyjnego należy kształtować w zgodzie z dokumentami UE i NATO oraz innymi inicjatywami międzynarodowymi, aby były one spójne i kompatybilne z systemami państw sojuszniczych oraz organizacji międzynarodowych, których członkiem jest Polska.

4.1. PODSYSTEM KIEROWANIA

42. Konieczne jest utworzenie i rozwijanie instytucji koordynującej działania prowadzone w ramach bezpieczeństwa informacyjnego we wszystkich sektorach bezpieczeństwa narodowego oraz budowanie zintegrowanego systemu przeciwdziałania zagrożeniom w środowisku informacyjnym.

43. Instytucja koordynująca powinna odpowiadać za realizację zadań związanych z bezpieczeństwem informacyjnym państwa, w tym:

- wypracowanie krajowej strategii przeciwdziałania zagrożeniom informacyjnym;
- zadania planistyczne w zakresie kierunków rozwoju polityki informacyjnej państwa;
- koordynację wysiłków zaangażowanych sektorów w kontekście szeroko rozumianej polityki informacyjnej państwa;
- integrację wysiłku informacyjnego sektora cywilnego i militarnego, w celu osiągnięcia efektu synergii działań;
- doskonalenie i rozwój teorii prowadzenia polityki informacyjnej państwa umożliwiającej zapewnienie realizacji interesów narodowych;
- konsolidowanie potencjału intelektualnego w zakresie działań informacyjnych;
- zapewnianie efektywnej płaszczyzny porozumienia i budowy dobrych praktyk w zakresie współpracy poszczególnych ogniw operacyjnych.

4.2. OGNIWA OPERACYJNE

44. Niezbędne jest stworzenie i rozwijanie mechanizmów (struktur wyposażonych w odpowiednie siły, środki i zdolności) adaptujących się do środowiska w razie konieczności reagowania na pojawiające się zagrożenia informacyjne, zdolnych do rozpoznania, analizy i oceny zagrożeń informacyjnych:

- rozbudowa narodowego systemu komunikacji strategicznej, w tym stworzenie instrumentów przeciwdziałania efektom agresji informacyjnej przeciwnika;
- implementacja zmian organizacyjno-strukturalnych oraz technicznych w zakresie walki informacyjnej;
- jasne określenie organów/jednostek/komórek - oraz ich kompetencji - odpowiedzialnych za utrzymanie stanu bezpieczeństwa informacyjnego, które będą rozliczane z określonych wyników (np. raporty z monitoringu);
- stworzenie struktur wewnątrz Sił Zbrojnych RP i rozwój ich zdolności w zakresie przeciwdziałania zagrożeniom hybrydowym (np. Centrum Operacji Komunikacyjnych), w szczególności rozwijanie zdolności planowania i kierowania oraz reakcji w zakresie walki informacyjnej, zarówno o charakterze ofensywnym, jak i defensywnym;
- powołanie zespołów funkcyjnych odpowiedzialnych za bieżące monitorowanie i odpowiednio szybkie reagowanie wobec powstających zagrożeń informacyjnych;
- rozwijanie zdolności służb specjalnych do prowadzenia w ramach wojen hybrydowych działań o charakterze informacyjnym, zarówno o charakterze ofensywnym, jak i defensywnym;
- budowa zdolności i narodowych struktur do przeciwdziałania zagrożeniom (operacje informacyjne i psychologiczne);
- rozwój zdolności w zakresie ochrony danych osobowych obywateli przed naruszeniami;
- budowa zdolności oddziaływania na grupy odbiorców w strefie wpływów potencjalnego agresora;
- zapewnienie spójności działań służących bezpieczeństwu informacyjnemu pomiędzy ogniwami wsparcia a pozostałymi ogniwami prowadzącymi operacje komunikacyjne.

45. Istnieje potrzeba wypracowania stosownych mechanizmów i procedur działania w zakresie bezpieczeństwa informacyjnego:

- opracowanie procedur planowania, organizowania, koordynacji i nadzoru w sferze bezpieczeństwa informacyjnego;
- opracowanie procedur działania oraz kompetencji poszczególnych organów na wypadek zagrożenia informacyjnego (w zakresie działań pasywnych i aktywnych);
- organizacja systemu szkolenia kadr w zakresie bezpieczeństwa informacyjnego.

46. Potrzebna jest optymalizacja działań informacyjnych w wymiarze międzynarodowym:

- rozwój zdolności polskiej dyplomacji w zakresie prowadzenia walki informacyjnej i promowania stanowiska Polski na formatach sojuszniczych;
- dostosowanie do standardów bezpieczeństwa informacyjnego wykorzystywanych przez organizacje międzynarodowe takie jak NATO i UE;
- opracowanie rozwiązań doktrynalnych spójnych z rozwiązaniami sojuszniczymi.

47. Potrzebne jest wypracowanie rozwiązań pozwalających na wykorzystanie potencjału mediów, sektora prywatnego i społeczeństwa obywatelskiego:

- wzmocnienie zdolności Ministerstwa Obrony Narodowej, Ministerstwa Kultury i Dziedzictwa Narodowego, Ministerstwa Edukacji Narodowej i Ministerstwa Nauki i Szkolnictwa Wyższego w zakresie realizacji zadań służących kształtowaniu postaw patriotycznych, proobronnych i propaństwowych oraz edukacji w zakresie ochrony praw człowieka i obywatela;

- utrzymanie i doskonalenie systemu narzędzi kształtowania świadomości społecznej, zgodnie z celami polityki informacyjnej państwa oraz interesem narodowym, w tym uruchomienie właściwych mechanizmów pozwalających dbać o poziom świadomości społecznej (spoty, media społecznościowe i inne formy przekazu);
- opracowanie procedur współpracy z mediami – bieżącej i w stanach zagrożenia – oraz opracowanie zasad/wytycznych doboru mediów w celu realizacji operacji komunikacyjnych wykorzystujących potencjał mediów masowych, a także współpracy z nimi w zakresie realizacji zadań z obszaru walki informacyjnej;
- zwiększenie efektywności przekazu informacyjnego i zaspokajania potrzeb informacyjnych mediów przez służby prasowe/informacyjne poszczególnych ogniw rządowych, w szczególności poprzez zacieśnienie współpracy administracji i służb z mediami;
- stworzenie i utrzymanie kanałów szybkiego dostępu do kluczowych mediów masowych w kraju i za granicą.

4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA

48. Istnieje potrzeba zapewnienia spójności działań służących bezpieczeństwu informacyjnemu pomiędzy ogniwami wsparcia a pozostałymi elementami prowadzącymi operacje komunikacyjne, dlatego konieczne jest zapewnienie mechanizmów współpracy międzyresortowej i partnerstwa publiczno-prywatnego w tym zakresie.

49. Potrzebne jest wypracowanie zasad, kierunków i form organizacyjnych edukacji dla bezpieczeństwa, kształtowania postaw patriotycznych, proobronnych, świadomości bezpieczeństwa narodowego, wsparcia dla inicjatyw społecznych, w tym budowy więzi Sił Zbrojnych RP i pozostałych struktur bezpieczeństwa ze społeczeństwem.

50. Istotnym elementem dbałości o bezpieczeństwo informacyjne RP jest wykorzystanie zdolności społeczeństwa do prowadzenia rozproszonych działań w zakresie walki informacyjnej w cyberprzestrzeni. Należy zadbać o rozwój społeczeństwa obywatelskiego i włączenie go do systemu bezpieczeństwa narodowego w zakresie walki informacyjnej poprzez:
    - zapobieganie zjawisku wykluczenia informacyjnego;
    - zaangażowanie społeczeństwa w kraju oraz Polonii w proces weryfikowania odbieranych przekazów informacyjnych;
    - opracowanie koncepcji budżetowej w zakresie wsparcia organizacji służących zapewnieniu tożsamości narodowej i dziedzictwa kulturowego, promujących postawy patriotyczne i proobronne w duchu polskiej racji stanu;
    - opracowanie planów i programów działania zmierzających do utrzymania odpowiedniej zdolności funkcjonowania społeczeństwa w czasie zagrożenia;
    - utworzenie katalogu inicjatyw kulturalnych wchodzących w skład przedsięwzięć wspierających politykę informacyjną państwa w duchu polskiego interesu narodowego.

51. Niezbędne jest promowanie rozwoju narodowej myśli technicznej w zakresie doskonalenia zdolności ochrony, obrony i rażenia w kontekście środowiska informacyjnego:
    - stymulowanie przez państwo rozwoju badań naukowych nad bezpieczeństwem;
    - utworzenie pozarządowej instytucji badawczej realizującej zadania własne, zlecenia organów i instytucji państwa oraz podmiotów publicznych w zakresie bezpieczeństwa narodowego (ukierunkowanych na kwestie bezpieczeństwa informacyjnego).

52. Potrzebne jest stworzenie silnego kanału komunikacyjnego do prowadzenia walki informacyjnej (m.in. na drodze przekształceń programowych TVP Polonia, wykorzystania Internetu itp.).

ZAKOŃCZENIE

53. Doktryna bezpieczeństwa informacyjnego RP – jako transsektorowy dokument wykonawczy do Strategii Bezpieczeństwa Narodowego RP – stanowi podstawę koncepcyjną do przygotowania i realizacji skoordynowanych w skali państwa działań dla bezpieczeństwa informacyjnego RP, sektora publicznego i sektora prywatnego.

54. Rekomendacje niniejszej Doktryny przeznaczone są do odpowiedniego wykorzystania przez wszystkie podmioty publiczne i prywatne odpowiedzialne za planowanie, organizowanie i realizowanie zadań w dziedzinie bezpieczeństwa informacyjnego.

55. Treść Doktryny powinna być rozwinięta przede wszystkim w kolejnej Polityczno-Strategicznej Dyrektywie Obronnej oraz w kolejnej edycji Strategii (Programu) Rozwoju Systemu Bezpieczeństwa Narodowego, a także w planach zarządzania kryzysowego oraz operacyjnych planach funkcjonowania struktur państwa w czasie zagrożenia i wojny, jak również w programach rozwoju sił zbrojnych i programach pozamilitarnych przygotowań obronnych.